## REMARKS

In the Office Action, claims 1-9 and 12-19 are rejected under 35 U.S.C. §112 as being indefinite, claims 1 and 3-9 are rejected under 35 U.S.C. §103(a) as being unpatentable over Ferchichi et al. in view of Gupta et al., claim 2 is rejected under 35 U.S.C. §103(a) as being unpatnetable over Ferchichi et al. and Gupta et al., and further in view of Wu, claim 10 is rejected under 35 U.S.C. §103(a) as being unpatnetable over Ferchichi et al. in view of Wu, claims 11-18 are rejected under 35 U.S.C. §103(a) as being unpatnetable over Ferchichi et al. and Wu, and further in view of Gupta et al.

In response to the office action, applicant believes that the teachings of the cited prior arts are significantly different from the instant invention, and respectfully contends that the rejection is unfounded. In the following analysis, the disclosure of Ferchichi et al., Gupta et al., and Wu as cited by the examiner will be discussed and compared with the instant invention to point out the difference.

Ferchichi (WO 01/60013 A1) discloses: a single sign-on module 13 (page 6, line 5) and a smart card 17 (page 6, line 9), which are respectively equivalent to the ICP and the user-login-identification means in Claim 1 of the present application; the single sign-on module 13 launches the user interface (arrow 11) in order to prompt the user for the login name and secrets (page 6, lines 13-15), which is equivalent to the recitation "the ICP adds an interface module in a login web page" in Claim 1 of the present application; the login name and the secrets entered are then checked in the single sign-on module 13 and compared with names and secrets stored in a protected memory area of the module 13 to verify the user's authorization. If the test fails, the user may be requested to try

again, until a predefined maximal number of tries has been reached (page 6, lines 19-26), which is only equivalent to the recitation "accesses the user-login-identification means via the interface module". However, **Claim 1 recites an additional step: "the ICP also provides an administration/drive module monitoring access of the user-login-identification means to set up a connection and hang up the connection of the user-login-identification means in the login web page" which is never been taught by Ferchichi**.

Ferchichi also discloses: another known example is the so-called SecureID authentication process. In this case, the user 10 is provided with a token that displays a new secret number each minute. At each authentication the user enters the new displayed number (page 8, lines 8-11), **which is different from the recitation "the user-login-identification means is provided with an ID number" in Claim 1 of the present application because the ID number of the instant invention is not a new secret number generated each minute**.

Ferchichi also discloses: the login name and the secrets entered are then checked in the single sign-on module 13 and compared with names and secrets stored in a protected memory area of the module 13 to verify the user's authorization. If the test fails, the user may be requested to try again, until a predefined maximal number of tries has been reached (page 6, lines 19-26). The examiner considers it as having disclosed the limitation "ICP access authentication information is stored in the user-login-identification means to verify whether the accessing ICP is authorized to access" in Claim 1 of the present application. However, the **login name** and **secrets** disclosed by Ferchichi is the

***user's identification information***, which is completely different from ***ICP access authentication information*** of the instant invention as recited in Claim 1. The ICP access authentication information refers to the ICP not the user. Therefore, Ferchichi does not disclose the recited limitation in Claim 1 of the present application.

Ferchichi also discloses: Figure 8 shows the authentication process for type AUTH1 authentication. In this case, the smart-card 17 just serves as a secure repository for authenticators. When the single sign-on module requests a login from an authentication server 110 of the type AUTH! (arrow 113), the latter replies by requesting an authenticator, usually a PIN or a password (arrow 114). The single sign-on module 13 requests this authenticator from the smart-card (arrow 111). If the latter is in active state, it sends the authenticator to the module 13 (arrow 112), possibly with other data. This authenticator is transmitted with other data to the server 110 (arrow 115); if the authenticator is verified, it sends the authentication results to the single sign-on module 13 (arrow 116) (page 12, lines 4-14), which the examiner considers as equivalent to the recitation "if the accessing ICP passed the verification, its access is permitted, otherwise the access is not permitted" in Claim 1 of the present application. However, in Ferchichi, **the single sign-on module 13 accesses the authentication server 110**, and **the smart-card 17 only serves as a secure repository for authenticators**. In contrast, in Claim 1 of the present application, **the ICP requests to access the user-login-identification means**. Therefore, the feature disclosed by Ferchichi is not equivalent to the recitation in Claim 1 of the present application.

Ferchichi also discloses: Figure 9 shows the authentication process for AUTH3

type authentication. In this case, the smart-card 17 is used to securely store the secret and to calculate the hash value derived from the stored secret. When the single sign-on module 13 requests a login from an authentication server 127 of the type AUTH3 (arrow 122), the latter replies by requesting an authenticator, usually the hash value of a PIN or password (arrow 123). The single sign-on module 13 requests this authenticator from the smart-card (arrow 120). If the latter is in active state, it computes the authenticator from the user password and possibly from other data and sends it to the module 13 (arrow 121), which sends it to the server 127 (arrow 124); if the authenticator is verified, the server 127 sends the authentication results to the single sign-on module 13 (arrow 125) (page 12, lines 15-27). The examiner regards the disclosure as teaching "the ICP is permitted to access the user-login-identification means only if the ICP is authenticated, when the user-login-identification means is activated". However, in Ferchichi, **the single sign-on module 13 accesses the authentication server 127**, and **the smart-card 127 is only used to securely store the secret and to calculate the hash value derived from the stored secret**. In contrast, in Claim 1 of the present application, the **ICP requests to access the user-login-identification means**. Therefore, the feature disclosed the Ferchichi is not equivalent to the recitation in Claim 1 of the present application.

In summary, difference between Claim 1 and Ferchichi resides in: the ICP also provides an administration/drive module monitoring access of the user-login-identification means to set up a connection and hang up the connection of the user-login-identification means in the login web page; the user-login-identification means is provided with an ID number; ICP access authentication information is stored in the user-

login-identification means to verify whether the accessing ICP is authorized to access; if the accessing ICP passed the verification, its access is permitted, otherwise the access is not permitted; the ICP is permitted to access the user-login-identification means only if the ICP is authenticated, when the user-login-identification means is activated; authenticating comprises, obtaining an authentication file via the interface module, transmitting the authentication file to the administration/drive module, decrypting the authentication file by the administration/drive module, and accessing the user-login-identification means.

Gupta (U.S. Pat Pub 2001/037469 A1) discloses: one or more authentication mechanism on the internet may utilize information/tool referred to as a "cookie"; Cookies are small pieces of information stored on individual's browsers that can later be read back from the browser. When a web site is accessed, a cookie may be sent by the web site identifying itself to the web browser (paragraph 35, lines 1-6), which is equivalent to the recitation "obtaining an authentication file via the interface module, transmitting the authentication file to the administration/drive module" in Claim 1 of the present application.

Gupta also discloses: the secure communication may provide that any information transmitted is encrypted prior to transmission (paragraph 86, lines 4-5), which is equivalent to the recitation "decrypting the authentication file by the administration/drive module" of Claim 1.

However, Gupta does not disclose: the ICP also provides an administration/drive module monitoring access of the user-login-identification means to set up a connection

and hang up the connection of the user-login-identification means in the login web page; the user-login-identification means is provided with an ID number; ICP access authentication information is stored in the user-login-identification means to verify whether the accessing ICP is authorized to access; if the accessing ICP passed the verification, its access is permitted, otherwise the access is not permitted; the ICP is permitted to access the user-login-identification means only if the ICP is authenticated, when the user-login-identification means is activated.

From the above analysis and comparison, it can be seen that many features recited in Claim 1 of the instant invention are not taught or suggested by either Ferchichi or Gupta, Therefore, it is not logical for a person skilled in this art to combine Ferchichi and Gupta to reach the instant invention, and the different features recited in Claim 1 are not obvious to persons skilled in the art. Applicant respectfully submits that Claim 1 should be allowable over Ferchichi et al. in view of Gupta et al. under 35 U.S.C. §103(a). By virtue of dependency, claims 2-9 should also be allowable.

Ferchichi discloses: a single sign-on process, and the process includes a mobile user with a mobile phone or with a laptop (abstract, lines 1-2), which is equivalent to the computer in Claim 10 of the present application; a single sign-on module (Figure 1, single sign-on module 13), which is equivalent to the ICP in Claim 10 of the present application; a smart-card (Figure 1, smart-card 17), which is equivalent to the user-login-identification means in Claim 10 of the present application; the login name and the secrets entered are then checked in the single sign-on module 13 and compared with names and secrets stored in a protected memory area of the module 13 to verify the user's

authorization (page 6, lines 19-22), which is equivalent to the recitation "the user-login-identification means is capable of accessing the computer from outside" in Claim 10 of the present application.

Ferchichi also discloses: the user 10 is prompted by the single sign-on module 13 at the beginning to enter a login name and a secret on a graphical user interface 160. This secret is used to activate the smart-card 17, and thus the smart-card will be able to process all authentications required thereafter for each other. **An external interface 161 forwards the authentication requests from the various authentication servers 162 to 169 to the single sign-on module 13, and sends back the retrieved authenticator from the smart-card 17 to those servers** (page 16, lines 17-24), which the examiner thinks is equivalent to the recitation "the computer can log in the Internet networks to communicate with different ICPs". However, in Ferchichi, **the mobile users communicate with different servers**; in Claim 10 of the present application, **the computer communicates with different ICPs**. Therefore, the feature disclosed by Ferchichi is not equivalent to the recitation in Claim 10 of the present application.

Ferchichi also discloses: to integrate PAP with the smart-card 17, the ID and password shall be stored in the EEPROM of the smart-card, the ID and password shall be stored in the EEPROM of the smart-card (page 22, lines 20-21), which the examiner considers as equivalent to the recitation "the user-login-identification has at least an identification number and encryption storage space". However, **in Ferchichi, the ID and password is the ID and password of the user, which is not the identification number of the user-login-identification means**. Furthermore, the EEPROM of the smart-card is

not encrypted. Therefore, the feature disclosed by Ferchichi is not equivalent to the recitation in Claim 10 of the present application.

Ferchichi also discloses: a one-way hash function 51 is used to ***transform*** the secret 50, together with some other data in an encrypted authenticator 52 (page 8, lines 21-23), which the examiner thinks is equivalent to the recitation "the user-login-identification means performs the information transmission by operating the computer". However, **Ferchichi means information *transformation*, not information *transmission***. Therefore, the feature disclosed by Ferchichi is not equivalent to the recitation in Claim 10 of the present application.

In summary, the difference between Claim 10 of the present application and Ferchichi lies in: the computer can log in the Internet networks to communicate with different ICPs; the user-login-identification has at least an identification number and encryption storage space; and the user-login-identification means performs the information transmission by operating the computer. These different features are not disclosed by Wu either. Therefore, applicant respectfully submits that Claim 10 should be allowable over the cited prior arts under 35 U.S.C. §103(a). By virtue of dependency, claims 11-18 should also be allowable.

From the foregoing discussion, it is clear that the instant invention differs from the cited prior arts. The physical difference results in different effects and is not obvious. Claims 1-18 should be allowable. The specification has been amended to correct a few editorial and grammatical errors. Prompt and favorable reconsideration of the application is respectfully solicited.

Respectfully submitted,

/Jason Z. Lin/

Jason Z. Lin
Agent for Applicant(s)
Reg. No. 37,492
Customer No. 33,804